Office/Contact: Division of Technology and Security
Source: SDBOR Policies 7:1 and 7:4
Link: https://www.sdbor.edu/policy/documents/7-1.pdf; https://www.sdbor.edu/policy/documents/7-4.pdf

SOUTH DAKOTA STATE UNIVERSITY
Policy and Procedure Manual

SUBJECT: Password Requirements
NUMBER: 7:6

1. Purpose

   This policy establishes the University's standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Policy

   a. All system-level passwords must be changed by the University designated responsible individual at a minimum on a yearly basis.

   b. All account user-level passwords must be changed at a minimum on a yearly basis.

   c. All passwords must contain a minimum of eight (8) characters.

   d. All passwords must be strong passwords, as defined below.

   e. General Password Construction Standards

      i. Strong passwords contain the following characteristics:

         1. Contain at least three (3) of the five (5) following character classes:
            a. Lower case characters
            b. Upper case characters
            c. Numbers
            d. Punctuation
            e. Special characters (e.g., !@#$%^&*()_+= etc.)

         2. Contain at least eight (8) alphanumeric characters

      ii. Weak passwords contain the following characteristics:

         1. Less than eight (8) characters

         2. Common words found in the dictionary

         3. Common usage words such as:
            a. Names of family, pets, friends, co-workers, etc.
            b. Birthdays and other personal information

c. Word or numbers patterns (e.g., qwerty, 12345, etc.)

f. Password Protection Standards

i. Passwords shall not be shared with anyone. Sharing or allowing another individual to use an account password is a violation of SDBOR Policy 7.1 and University Policy 7:5, (Acceptable Use Policy). All passwords are to be treated as sensitive, confidential information.

1. The University Support Desk, as a function of operation, may ask users for their passwords for technical support services. These instances do not violate SDBOR Policy 7:1 or University Policy 7:5.

ii. Passwords must never be written down or stored online without encryption.

iii. Passwords must not be revealed in email, chat, or other electronic communication.

iv. Passwords must not be revealed on questionnaires or security forms.

v. Vendor password sharing must be approved by the Division of Technology and Security.

vi. The Division of Technology and Security may require more restrictive policy standards as circumstances require.

vii. If someone demands a password, individuals should refer them to this policy and direct them to the Division of Technology and Security.

g. If an account or password compromise is suspected, incidents must be immediately reported to the Division of Technology and Security. The Division of Technology and Security will not send or request individuals a password by email, and individuals should not respond to such requests.

3. Responsible Administrator

The Vice President for Technology & Security, or designee, is responsible for the annual and ad hoc review of this policy and its procedures. The University President is responsible for formal policy approval.

SOURCE: Approved by President 11/17/2015.